FBI Tools/Methods

FBI Pre-deployment Checklist for Cyber Investigations

INVESTIGATIVE TOOLS

The following investigative tools are available during incident response:

Investigative Interviews (subject, victim, witness)
The FBI can conduct interviews to gather information and evidence for an investigation.

Evidence Collection (technical and physical)
The FBI has the ability to collect evidence. This includes the ability to obtain forensic images of computer systems. The FBI utilizes its Computer Analysis Response Team (CART) program for collecting digital evidence.

Electronic Surveillance (consent, court-ordered, etc.)
The FBI has the ability, with proper legal authority, to conduct electronic surveillance.

Investigative Analysis
Cyber FBI agents and analysts are trained to conduct technical analysis in the field. This includes e-mail header analysis, network traffic analysis, and intrusion analysis. The FBI has specific units at FBI Headquarters to assist with highly technical or specialized analytical requests.

Malware analysis
The FBI developed a system called the Binary Analysis, Characterization, and Storage System (BACSS) which is used to triage malware identified in FBI investigations. Through this system, the FBI has the ability to cross-correlate malware events. If malware requires further, in-depth analysis, the FBI has specific units at FBI Headquarters to assist with this specialized analytical request.

Cyber Action Team (CAT) Deployment
The mission of the CAT is to deploy globally at the direction of Cyber Executive Management, in order to bring in-depth cyber expertise, specialized investigative skills, and direct connectivity to those cyber initiatives, investigations, and emergencies deemed critical and significant. These incidents are aligned with the FBI's national priorities, and are defined primarily as intrusions into government, military, and commercial systems that have a direct and adverse effect on the national information infrastructure.

Legal Attaché Support
The FBI has Legal Attachés or LEGATS throughout the world to support the FBI’s mission. These LEGATS foster strategic partnerships to local law enforcement, intelligence, and security services agencies to facilitate information exchange and exploring joint operational opportunities.

National Cyber Investigative Joint Task Force (NCIJTF)

The NCIJTF is the national focal point for the U.S. government for the coordination, integration, and sharing of information related to all domestic cyber threat investigations. The NCIJTF is an alliance of peer agencies with complementary missions to protect national cyber interests as well as the political, economic, and overall vitality of our nation. Assignees from participating agencies have access to a unique, comprehensive view of the nation's cyber situation while working together in a collaborative environment in which they maintain the authorities and operational/investigative responsibilities of their represented agencies.

Access to Legal Process

The FBI has access to legal process which can authorize subpoenas, search warrants, indictments, arrests, etc. In addition to legal process, the FBI can work through consent to obtain information or evidence in support of the investigation.

Review Current Field Office Collections and Investigations

The FBI has 56 field offices working cyber investigations. The combined information from all field office investigations offers an in-depth view of a threat not readily available through other databases.

PRE-DEPLOYMENT CHECKLIST

Prior to the FBI responding to a cyber incident, the items in the following checklist would greatly enhance the FBI's ability to effectively further the investigation.

Network Inventory

Victims should provide as much information as possible regarding the inventory of computer systems and network components (i.e., workstations, servers, routers, switches, etc).

Software Inventory

Victims should provide as much information as possible regarding the inventory of software applications used in the organization (i.e., operating systems, application versions, proprietary applications).

Up-To-Date Network Topology Maps

Network topology maps should provide a current, functional understanding of the organization's network.

Network- and Host-Based Incident Logs

These logs include, but are not limited to, web, proxy, IDS, VPN, DNS, database, remote access, and firewall logs.

Forensic Images of Compromised Hosts

If possible and your organization has the capability, obtain forensic images of identified compromised hosts. It is also recommended your organization maintains a log of activity for reference.

List of External and Internal IP Addresses

This list should include DNS, web server, proxies and workstations.

Physical Access Logs

These logs typically include video logs from security cameras, entry/exit access logs, keycard logs, and two-factor authentication logs.

Legal Banner and Computer Use Agreement

These legal items are essential to assure the data can legally be passed to the FBI.

Domain Infrastructure, Group Policy Hierarchy, and Access Control Details

These items can typically be provided by network/system administrators.